A method of enciphering quantum states

Hiroo Azuma[*]

Mathematical Engineering Division, Canon Research Center,

5-1, Morinosato-Wakamiya, Atsugi-shi, Kanagawa, 243-0193, Japan

E-mail: hiroo@crc.canon.co.jp

Masashi Ban

Advanced Research Laboratory, Hitachi Ltd.,

Hatoyama, Saitama, 350-0395, Japan

E-mail: m-ban@harl.hitachi.co.jp

December 2, 2000

Abstract

In this paper, we propose a method of enciphering quantum states of two-state systems (qubits) for sending them in secrecy without entangled qubits shared by two legitimate users (Alice and Bob). This method has the following two properties. First, even if an eavesdropper (Eve) steals qubits, she can extract information from them with certain probability at most. Second, Alice and Bob can confirm that the qubits are transmitted between them correctly by measuring a signature. If Eve measures m qubits one by one from n enciphered qubits and sends alternative ones (the Intercept/Resend attack), a probability that Alice and Bob do not notice Eve's action is equal to $(3/4)^m$ or less. Passwords for decryption and the signature are given by classical binary strings and they are disclosed through a public channel. Enciphering classical information by this method is equivalent to the one-time pad method with distributing a classical key (random binary string) by the BB84 protocol. If Eve takes away qubits, Alice and Bob lose the original quantum information. If we apply our method to a state in iteration, Eve's success probability decreases exponentially. We cannot examine security against the case that Eve makes an attack with using entanglement. This remains to be solved in the future.

1 Introduction

Since considerable progress was made in quantum information and computation theory, many researchers have been studying to realize the information processing that we have

---

[*]Present address: Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, UK. E-mail: hiroo.azuma@qubit.org

never had by using quantum mechanics[16]. At the same time, it has been studying to apply the uncertainty principle, the quantum no-cloning theorem, and entanglement between quantum systems to cryptography[8]. The BB84 protocol is considered to be an effective method for the key distribution. By combining it with the one-time pad method, we obtain a highly secure cryptography[1][2][5]. On the other hand, the quantum teleportation is considered to be an excellent method for sending arbitrary quantum states between two parties[6][7].

The BB84 protocol is used for a secure distribution of a classical key (binary string) to two legitimate users (Alice and Bob). Choosing a basis vector at random from four basis vectors, the rectilinear basis $\{|0\rangle, |1\rangle\}$ and the circular basis $\{(1/\sqrt{2})(|0\rangle \pm |1\rangle)\}$, as a state of a photon (a two-state system or a qubit), Alice sends it to Bob. Bob measures a transmitted photon in an orthonormal basis that he chooses from two bases (rectilinear and circular) at random and independently of Alice.

Not being consistent with each other, the rectilinear basis and the circular basis are called conjugate bases. A result of measurement with a wrong basis is random. If an eavesdropper (Eve) steals a photon from the channel, measures it in a basis chosen at random, and sends an alternative one, Alice and Bob find inconsistency with probability of 1/4 or more and notice Eve's eavesdropping. In this way, by using the uncertainty principle, the BB84 protocol reveals Eve's illegal act.

A. K. Ekert proposed another protocol for distributing a classical key by transmitting pairs of qubits in EPR states, $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$, apart to Alice and Bob from a source[3]. They detect Eve by Bell's theorem. Considering a simplified protocol of A. K. Ekert's, C. H. Bennett et al. showed it was equivalent to BB84[4]. From these successive works, it has been recognized that we do not need to use the entanglement for distributing a classical key by quantum mechanics. (But, by combining entanglement purification protocol with Ekert's protocol, we can distribute a classical key in high secrecy[9].)

The quantum teleportation is used for transmitting an arbitrary state from Alice to Bob. They share an EPR-pair of qubits beforehand. Alice carries out the Bell-measurement on both a one-qubit state $|\psi\rangle$ that she wants to send and her qubit of the EPR-pair. Receiving a result of her measurement, Bob can construct $|\psi\rangle$ from his qubit of the EPR-pair. A characteristic of this method is that classical information and non-classical information of $|\psi\rangle$ are divided perfectly and only the classical information is sent through the public channel. If they share the EPR-pair correctly, Eve can neither eavesdrop on the state nor destroy it in principle.

These methods are related to the quantum no-cloning theorem. It tells us there is no unitary transformation that makes accurate clones of arbitrary quantum states[8]. In the BB84 protocol, it gives an effect as follows. Not knowing which basis is chosen for a qubit (photon) that she extracts from the quantum channel, rectilinear or circular, Eve cannot make a clone of the qubit and keep it. What she can do is only measuring the qubit in a proper basis and sending an alternative one that depends on a result of the measurement to Bob. In the quantum teleportation, the following thing is important. Because Alice can neither measure $|\psi\rangle$ without disturbance nor make an accurate clone of it, she cannot extract information from $|\psi\rangle$ at all. During the whole process, Alice and Bob have no knowledge about $|\psi\rangle$.

In the quantum teleportation, Alice and Bob have to share an EPR-pair of qubits beforehand. After being emitted by a source, this pair flies towards them apart through a quantum channel. Therefore, for example, if Eve takes away the qubit that Bob is supposed to have and sends an alternative one to him, she succeeds in eavesdropping. To avoid such a trouble, Alice and Bob need to share a lot of EPR-pairs and to purify them[9].

In this paper, we consider a method for enciphering arbitrary quantum states for sending them in secrecy without entangled qubits shared by Alice and Bob beforehand. In our method, there are two points as follows. (See Figure 3.)

First, even if Eve takes away qubits, she can extract quantum information from them with certain probability at most. (If Eve measures m qubits one by one from n enciphered qubits and sends alternative ones, a probability that Alice and Bob do not notice Eve's act is equal to $(3/4)^m$ or less. We assume Eve makes only the Intercept/Resend attack[2].) Alice applies a unitary operator U_i which is chosen at random from a set of operators $\mathcal{M} = \{U_j\}$ to an arbitrary n-qubit state $|\Psi\rangle$ that she wants to send in secrecy. The subscript i of U_i is a password for decryption. Not knowing which operator is chosen from $\mathcal{M}$, Eve regards the enciphered state as a mixed state of $U_j|\Psi\rangle$ for all $U_j \in \mathcal{M}$ with equal probability. If Alice prepares $\mathcal{M}$ so that the density operator of the mixed state may be in proportion to the identity operator $\boldsymbol{I}$, Eve cannot extract the information of $|\Psi\rangle$ at all without the password i. The reason of this is that even if Eve puts auxiliary qubits on the density operator $\rho = (1/2^n)\boldsymbol{I}$, applies unitary transformations to it, or measures it, she cannot extract $|\Psi\rangle$. After confirming that the quantum state is transmitted correctly, Alice releases the password i in our protocol. Therefore, to extract information from $|\Psi\rangle$, Eve has to eavesdrop without disturbing Alice and Bob's certification process. (This technique has been also discussed by P. O. Boykin and V. Roychowdhury, and M. Mosca et al.[17]. They have shown the following result. When we define $\mathcal{M}$ as a set of tensor products of the Pauli matrices, the number of the operators $\{U_i\}$ gets minimum and the subscript i is represented by a $2n$-bit string.)

Second, Alice and Bob can confirm that a quantum state received by Bob is a genuine one sent by Alice. Not having knowledge about the n-qubit state $|\Psi\rangle_Q$ at all, they do not notice Eve replace the genuine qubits with alternative ones. Therefore, they need to confirm that the qubits Bob receives are genuine. (It seems like authentication of the identity of a correspondent on networks.) In our method, after putting an n-qubit state $|a\rangle_S$ ($a \in \{0,1\}^n$) that represents her signature on $U_i^Q|\Psi\rangle_Q$, Alice makes entanglement between qubits of each pair in the system Q and S. Here, we call the quantum system which represents the transmitted information Q and the quantum system which represents the signature S. Then, to forbid Eve to make clones of qubits, Alice applies an operator chosen at random from $\mathcal{L} = \{\boldsymbol{I}, H, \sigma_x, H\sigma_x\}$ to each qubit, where H is called the Hadamard transformation and it causes $|0\rangle \to (1/\sqrt{2})(|0\rangle + |1\rangle)$, $|1\rangle \to (1/\sqrt{2})(|0\rangle - |1\rangle)$, and σ_x is one of the Pauli matrices and it causes $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$. Hence, quantum information of each qubit is encoded in a basis chosen at random from two conjugate bases (rectilinear and circular). Therefore, if Eve does anything on the qubits, Alice and Bob can find inconsistency and detect Eve with certain probability. This is essentially the same technique used in BB84. In our method, certification of a correspondent and detection of Eve are done at the same time. The second password for

decryption is which operators are chosen from $\mathcal{L}$.

Because the passwords and the signature represented by classical binary strings are transmitted by the public channel, Eve also knows them. If $|\Psi\rangle_Q$ represents classical information (a product state of $|0\rangle$ and $|1\rangle$), our protocol is equivalent to the one-time pad method with classical key distribution by BB84.

If Alice and Bob apply our enciphering method to a state in iteration, a probability that Eve gets quantum information with fidelity of 1 decreases exponentially. (If they encipher a one-qubit state with N qubits, the probability is given by $(3/4)^{N/2}$.) We can regard it as privacy amplification process. We cannot examine security against the case that Eve makes an attack with using entanglement. This remains to be solved in the future.

This paper is organized as follows. In Sec. 2, we explain how Alice and Bob forbid Eve to extract the original quantum information and how they confirm the qubits are transmitted correctly. In Sec. 3, we explain the whole protocol and discuss how Bob confirms that he receives qubits. In Sec. 4, we discuss security of our protocol against Eve's Intercept/Resend attack on each qubit. In Sec. 5, we discuss privacy amplification process. In Sec. 6, we give a brief discussion.

2   Enciphering quantum states

In this section, we explain how Alice and Bob forbid Eve to extract the original quantum information and how they confirm the qubits are transmitted correctly.

First, we consider transforming an arbitrary quantum state so that Eve cannot recover an original quantum state. For simplicity, we consider an arbitrary one-qubit state for a while and we describe its density operator as ρ defined on a two-dimensional Hilbert space $\mathcal{H}_2$. We assume Alice wants to send ρ to Bob in secrecy. She does not know ρ at all, because her partial measurement destroys it.

Alice prepares a set of operators,

$$\mathcal{M} = \{\sigma_j : j = 0, x, y, z\},$$

where $\sigma_0 = \boldsymbol{I}$ (the identity operator) and $\{\sigma_x, \sigma_y, \sigma_z\}$ are the Pauli matrices. Taking

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

for an orthonormal basis, we write them as

$$\boldsymbol{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$\mathcal{M}$ may be disclosed in public. Choosing an operator σ_i from $\mathcal{M}$ at random, Alice carries out the following unitary transformation,

$$\rho \rightarrow \sigma_i \rho \sigma_i^\dagger.$$

4

She keeps the subscript i secret as a password and never tells it to anyone. Because the subscript takes a value from $\{0, x, y, z\}$, the password can be represented by 2-bit classical information.

Not knowing which transformation Alice applies to the qubit, Eve has to regard the state as

$$\rho' = \frac{1}{4} \sum_{j=0,x,y,z} \sigma_j \rho \sigma_j^\dagger.$$

Generally, the density operator ρ satisfies $\rho^\dagger = \rho$, $\mathrm{Tr}\rho = 1$, $0 \leq \lambda_1 \leq 1$, $0 \leq \lambda_2 \leq 1$, and $\lambda_1 + \lambda_2 = 1$ where λ_1, λ_2 are eigenvalues of ρ. Hence, we can describe an arbitrary ρ as

$$\rho = \frac{1}{2}(\boldsymbol{I} + \boldsymbol{a} \cdot \boldsymbol{\sigma}),$$

where $\boldsymbol{a} = (a_1, a_2, a_3)$ is a three-component real vector and $0 \leq \sum_{k=1}^{3} a_k^2 \leq 1$. Because

$$\rho' = \frac{1}{2}\boldsymbol{I} + \frac{1}{8} \sum_{j=0,x,y,z} \boldsymbol{a} \cdot \sigma_j \boldsymbol{\sigma} \sigma_j^\dagger, \tag{1}$$

and

$$\sigma_j \sigma_k \sigma_j = \begin{cases} \sigma_k & j = 0 \text{ or } j = k \\ -\sigma_k & j \neq k \text{ and } j, k \in \{x, y, z\} \end{cases},$$

there is no contribution from the second term of Eq. (1). We obtain

$$\rho' = \frac{1}{2}\boldsymbol{I}.$$

Therefore, even if Eve takes away ρ', she cannot extract information from it at all, because she does not know the password i.

An arbitrary n-qubit density operator ρ_n is given by

$$\rho_n = \frac{1}{2^n}\left(\boldsymbol{I} + \sum_{\boldsymbol{k} \in \{0,x,y,z\}^n, \boldsymbol{k} \neq (0,\cdots,0)} a_{\boldsymbol{k}} U_{\boldsymbol{k}}\right), \tag{2}$$

where

$$U_{\boldsymbol{k}} = \sigma_{k_1} \otimes \cdots \otimes \sigma_{k_n},$$

and $a_{\boldsymbol{k}}$ ($\boldsymbol{k} \in \{0, x, y, z\}^n$, $\boldsymbol{k} \neq (0, \cdots, 0)$) is real. (In Eq. (2), $\boldsymbol{I}$ represents the identity operator for n-qubit states.) Choosing an operator $U_{\boldsymbol{i}}$ from

$$\mathcal{M}_n = \{U_{\boldsymbol{k}} : U_{\boldsymbol{k}} = \sigma_{k_1} \otimes \cdots \otimes \sigma_{k_n}, \boldsymbol{k} \in \{0, x, y, z\}^n\},$$

at random, Alice applies it to ρ_n for encryption as $\rho_n \rightarrow U_{\boldsymbol{i}}\rho_n U_{\boldsymbol{i}}^\dagger$. If Eve takes away the density operator given by

$$
\begin{aligned}
\rho_n' &= \frac{1}{4^n} \sum_{\boldsymbol{j} \in \{0,x,y,z\}^n} U_{\boldsymbol{j}}\rho_n U_{\boldsymbol{j}}^\dagger \\
&= \frac{1}{2^n}\boldsymbol{I} + \frac{1}{4^n \cdot 2^n} \sum_{\boldsymbol{j},\boldsymbol{k} \in \{0,x,y,z\}^n, \boldsymbol{k} \neq (0,\cdots,0)} a_{\boldsymbol{k}} U_{\boldsymbol{j}} U_{\boldsymbol{k}} U_{\boldsymbol{j}}^\dagger \\
&= \frac{1}{2^n}\boldsymbol{I}, \tag{3}
\end{aligned}
$$

Figure 1: The second encryption by Alice.

$x_k, a_k \in \{0, 1\}$

$L_{k,1}{}^Q, L_{k,2}{}^S \in \{\boldsymbol{I}, H, \sigma_x, H\sigma_x\}$
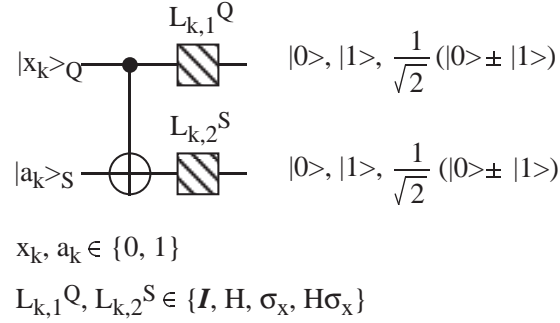
she cannot extract information from ρ'_n at all. Even if she puts auxiliary systems on ρ'_n, applies unitary transformations to it, or carries out measurements, she cannot obtain ρ_n. The password of $\boldsymbol{i}$ is given by a $2n$-bit string. (This technique is also discussed by P. O. Boykin and V. Roychowdhury, and M. Mosca et al. as mentioned in Sec. 1[17].)

Next, we explain how Alice and Bob confirm that the qubits are transmitted between them correctly. If Eve takes away ρ'_n and sends an alternative state $\tilde{\rho}_n$ to Bob, he carries out the inverse operation on the state that he receives as $\tilde{\rho}_n \rightarrow U_{\boldsymbol{i}}\tilde{\rho}_n U_{\boldsymbol{i}}^{\dagger}$. Not having knowledge about the original ρ_n at all, Alice and Bob do not notice what Bob gets is a fake.

To avoid this trouble, they put a signature on ρ_n. Reading it, they can confirm that Bob receives the state transmitted from Alice correctly. It is important that Eve cannot change the signature. For simplicity, we describe the state as a ket vector $\forall |\Psi\rangle_Q \in \mathcal{H}_2^n$ instead of the density operator ρ_n for a while. If the n-qubit state is given by a mixed state, we can give a similar discussion. We call the system that represents the quantum information Q and the system that represents the signature S.

Preparing an n-bit random string $\forall \boldsymbol{a} = (a_1, \cdots, a_n) \in \{0,1\}^n$ as her signature, Alice attaches a qubit $|a_k\rangle_S$ to the kth qubit of

$$U_{\boldsymbol{i}}^Q |\Psi\rangle_Q = \sum_{\boldsymbol{x} \in \{0,1\}^n} c_{\boldsymbol{x}} |x_1\rangle \cdots |x_n\rangle \in \mathcal{H}_2^n. \tag{4}$$

Applying the controlled-NOT (C-NOT) gate to the kth pair as Figure 1, she obtains

$$|x_k\rangle_Q |a_k\rangle_S \rightarrow |x_k\rangle_Q |a_k \oplus x_k \bmod 2\rangle_S \qquad \text{for } k = 1, \cdots, n.$$

Choosing $L_{k,1}^Q, L_{k,2}^S \in \mathcal{L} = \{\boldsymbol{I}, H, \sigma_x, H\sigma_x\}$ at random, she applies them to the qubits of the pair, where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Alice repeats this operation on the $k = 1, \cdots, n$th qubit, and we write the whole transformation as $V_{\boldsymbol{\alpha}}^{QS}$. $\boldsymbol{\alpha}$ represents which operators are chosen from $\mathcal{L}$. The second password $\boldsymbol{\alpha}$ is given by a classical $4n$-bit string.

Figure 2: Typical quantum gates.

(i) controoled-NOT gate   (ii) σ_x gate

$i, j \in \{0, 1\}$
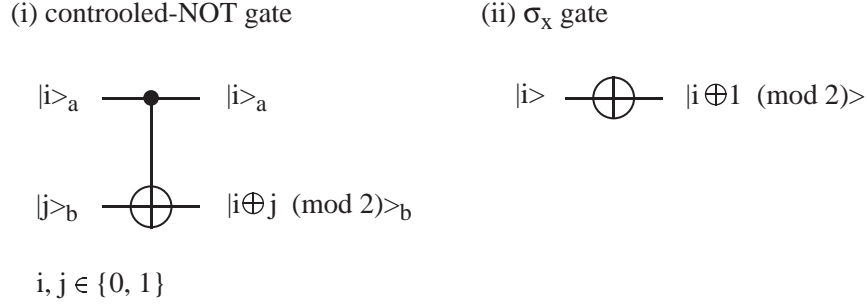
We often describe successive operations on qubits as a network like Figure 1. A horizontal line represents a qubit and time proceeds from left to right. Figure 2 shows examples of unitary transformations applied to qubits. Figure 2. i and ii. represent the C-NOT gate and σ_x each[10].

The operations that we have discussed are summarized as follows,

$$
\begin{aligned}
|\Psi\rangle_Q &\rightarrow U_i^Q |\Psi\rangle_Q && \text{(1st password } \boldsymbol{i}) \\
&\rightarrow |\boldsymbol{a}\rangle_S \otimes U_i^Q |\Psi\rangle_Q && \text{(signature } \boldsymbol{a}) \\
&\rightarrow V_{\boldsymbol{\alpha}}^{QS} [|\boldsymbol{a}\rangle_S \otimes U_i^Q |\Psi\rangle_Q] && \text{(2nd password } \boldsymbol{\alpha}).
\end{aligned}
$$

Double encryption prevents Eve from using $|\boldsymbol{a}\rangle_S$ ill. If $V_{\boldsymbol{\alpha}}^{QS}$ is not applied to the state, Eve may take away all of the qubits, keep $U_i^Q |\Psi\rangle_Q$, and send a fake of $|\boldsymbol{a}\rangle_S \otimes |\tilde{\Psi}\rangle_Q$ to Bob.

If Eve does anything on the kth qubit of Q, the signature of $|a_k\rangle_S$ is destroyed and Bob fails in the certification process with certain probability or more. This is caused by the facts that conjugate bases chosen at random represent the systems Q and S, and there is entanglement between Q and S. If she does anything on the kth qubit of S, we can get a similar result. We estimate a probability that Alice and Bob notice Eve's illegal act in Sec. 4.

3 The protocol for secure transmission

We consider a protocol for transmitting an arbitrary quantum state $\forall |\Psi\rangle_Q \in \mathcal{H}_2^n$ from Alice to Bob in secrecy against Eve's eavesdropping by using the encryption method discussed in the previous section. Alice and Bob do not have knowledge about $|\Psi\rangle_Q$ at all. Both of them can use the following two channels.

- The classical channel: It transmits classical binary strings in public. Eve can make accurate copies of them, but she cannot alter them.

- The quantum channel: It transmits sequences of qubits (quantum information). Eve can interact with them, but she cannot make accurate copies of them.

Alice sends qubits to Bob according to the following protocol. (See Figure 3.)

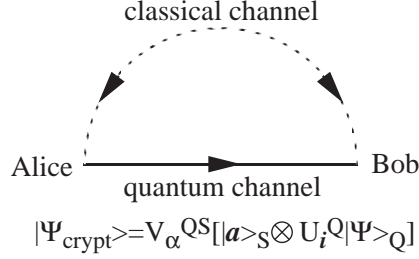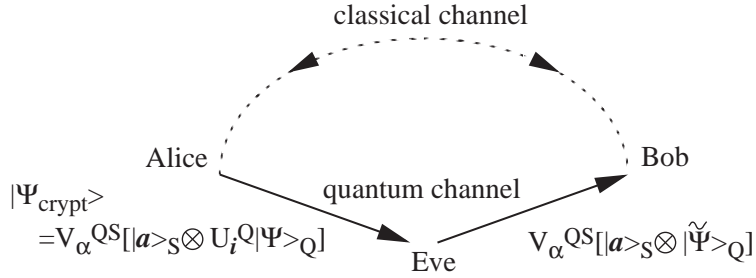Figure 3: Secure transmission between Alice and Bob.

classical channel

Alice ——→ Bob
quantum channel

$|\Psi_{\mathrm{crypt}}\rangle = V_\alpha^{QS}[|a\rangle_S \otimes U_i^Q|\Psi\rangle_Q]$

Figure 4: Eve's strategy for eavesdropping.

classical channel

Alice   Bob

$|\Psi_{\mathrm{crypt}}\rangle$ quantum channel

$= V_\alpha^{QS}[|a\rangle_S \otimes U_i^Q|\Psi\rangle_Q]$ $V_\alpha^{QS}[|a\rangle_S \otimes |\widetilde{\widetilde{\Psi}}\rangle_Q]$

Eve

1. Alice sends $|\Psi_{\mathrm{crypt}}\rangle \equiv V_{\boldsymbol\alpha}^{QS}[|\boldsymbol a\rangle_S \otimes U_{\boldsymbol i}^Q|\Psi\rangle_Q]$ of $2n$ qubits to Bob through the quantum channel.

2. Receiving $2n$ qubits, Bob breaks off the quantum channel and reports arrival of them to Alice through the classical channel.

3. Receiving the report from Bob, Alice tells Bob what transformation $V_{\boldsymbol\alpha}^{QS}$ is through the classical channel. (She discloses the $4n$-bit password $\boldsymbol\alpha$.)

4. Applying $V_{\boldsymbol\alpha}^{QS\dagger}$ to the state that he has received and measuring the signature, Bob tells Alice a result of the measurement (an n-bit string) through the classical channel.

5. Receiving the n-bit string from Bob, Alice examines whether it coincides with the signature $\boldsymbol a$ or not. If it coincides with her original signature, she tells Bob what transformation $U_{\boldsymbol i}^Q$ is through the classical channel. (She discloses the $2n$-bit password $\boldsymbol i$.) If it does not coincide, she concludes Eve has eavesdropped on qubits and stops the protocol.

6. Bob applies $U_{\boldsymbol i}^{Q\dagger}$ to the state that he has and obtains the original state $|\Psi\rangle_Q$.

In this protocol, it is important that Bob confirms the arrival of $2n$ qubits ($|\Psi_{\mathrm{crypt}}\rangle$ or Eve's fake) and breaks off the quantum channel at the second step. To understand the reason of this, we assume the following case. (See Figure 4.) Although $|\Psi_{\mathrm{crypt}}\rangle$ is still halfway on the channel, Bob reports the arrival of qubits to Alice by mistake, and she

discloses $V_{\boldsymbol{\alpha}}^{QS}$ through the classical channel. Eve may take away $|\Psi_{\text{crypt}}\rangle$, apply $V_{\boldsymbol{\alpha}}^{QS\dagger}$ to it, and obtain $|\boldsymbol{a}\rangle_S \otimes U_{\boldsymbol{i}}|\Psi\rangle_Q$ before Bob receives qubits. Eve can keep $U_{\boldsymbol{i}}|\Psi\rangle_Q$, combine a false state $|\tilde{\Psi}\rangle_Q$ with $|\boldsymbol{a}\rangle_S$, and send $V_{\boldsymbol{\alpha}}^{QS}[|\boldsymbol{a}\rangle_S \otimes |\tilde{\Psi}\rangle_Q]$ to Bob. If the quantum channel is still open, Bob receives $V_{\boldsymbol{\alpha}}^{QS}[|\boldsymbol{a}\rangle_S \otimes |\tilde{\Psi}\rangle_Q]$. Because the signature is correct, Alice and Bob cannot notice Eve's illegal act. Alice discloses $U_{\boldsymbol{i}}^Q$ in public and finally Eve gets $|\Psi\rangle_Q$.

To avoid this trouble, Bob needs to verify that a batch of qubits ($|\Psi_{\text{crypt}}\rangle$ or Eve's fake) has arrived. For example, it is good for Bob to take the following method.

We construct a qubit from a pair of optical paths (modes) that are represented by x and y in Figure 5. iii[11]. We describe a state that there is no photon on a mode as $|0\rangle$ and a state that there is a photon on a mode as $|1\rangle$. Writing a state that no photon is on the mode x and one photon is on the mode y as $|0\rangle_x \otimes |1\rangle_y = |01\rangle$, we regard $|01\rangle$ as logical $|\bar{0}\rangle$. We regard $|1\rangle_x |0\rangle_y$ as logical $|\bar{1}\rangle$ similarly. Hence, we can write an arbitrary state of a qubit as

$$|\psi\rangle = \alpha|01\rangle + \beta|10\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \qquad \text{for } |\alpha|^2 + |\beta|^2 = 1.$$

We assume Eve puts a 50-50 beamsplitter halfway on the quantum channel to take away photons. A state of a photon is a superposition of a state that it is on the side of Bob and a state that it is on the side of Eve with amplitude $1/\sqrt{2}$ each,

$$\frac{1}{\sqrt{2}}|\text{photon on the side of Bob}\rangle + \frac{1}{\sqrt{2}}|\text{photon on the side of Eve}\rangle.$$

To examine whether the qubit of $|\psi\rangle$ has come on his own side or not, Bob prepares another auxiliary photon and applies nonlinear interaction between the logical photon on the mode x or y and the auxiliary one. On an optical system of Figure 5. iii, if the photon counter D_a detects the auxiliary photon, the logical photon is projected into the state that it is on the side of Bob. On the other hand, D_b's detection projects the logical photon into the state that it is on the side of Eve.

In Figure 5. iii, there are beamsplitters B which apply $SU(2)$ transformations to logical kets $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ as Figure 5. i, and Kerr-type devices K which induce nonlinear interactions between two incoming photons as Figure 5. ii. The device K shifts a phase of a wave function by π only if a pair of photons comes into it. (Q. A. Turchette et al. succeeds in shifting the phase by $\Delta \sim 16°$[12].)

To clarify the operation of Figure 5. iii, we describe it by a network of quantum gates in Figure 6[13]. Assuming the first and the second qubits are in an arbitrary entangled state $|\Psi\rangle_Q$, we examine whether the first qubit exists or not by measuring an auxiliary qubit system A. When we write the whole system as
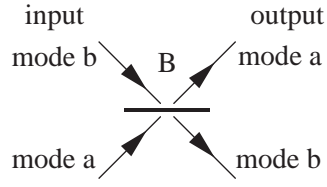
$$|\Psi\rangle_Q|0\rangle_A = \sum_{i,j \in \{0,1\}} c_{ij}|i\rangle_2|j\rangle_1|0\rangle_A,$$

$|\Psi\rangle_Q|0\rangle_A$ is transformed as follows in Figure 6,

$$|\Psi\rangle_Q|0\rangle_A = \sum_i (c_{i0}|i\rangle_2|0\rangle_1 + c_{i1}|i\rangle_2|1\rangle_1)|0\rangle_A$$

$$\xrightarrow{\text{step 1}} \sum_i (c_{i0}|i\rangle_2|1\rangle_1|0\rangle_A + c_{i1}|i\rangle_2|0\rangle_1|1\rangle_A)$$

9

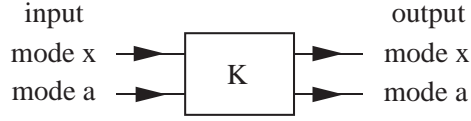Figure 5: The photon counting measurement with nonlinear optical devices.

(i)
50-50 beamsplitter

input   output
mode b $\diagdown$ B $\diagup$ mode a

mode a $\diagup$ $\diagdown$ mode b

$B : |1>_a|0>_b \longrightarrow \frac{1}{\sqrt{2}}(|1>_a|0>_b - |0>_a|1>_b)$

$|0>_a|1>_b \longrightarrow \frac{1}{\sqrt{2}}(|1>_a|0>_b + |0>_a|1>_b)$

(ii)
Kerr-type quantum phase-gate

input   output
mode x $\longrightarrow$ $\boxed{K}$ $\longrightarrow$ mode x
mode a $\longrightarrow$ $\longrightarrow$ mode a

$K : |1>_x|0>_a \longrightarrow |1>_x|0>_a$

$|0>_x|1>_a \longrightarrow |0>_x|1>_a$

$|1>_x|1>_a \longrightarrow -|1>_x|1>_a$

(iii)
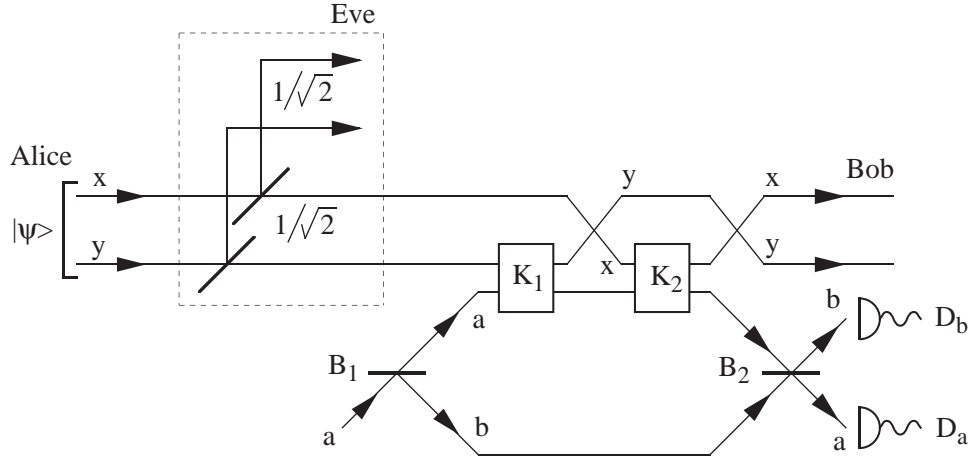
Figure 6: A quantum network for photon counting.
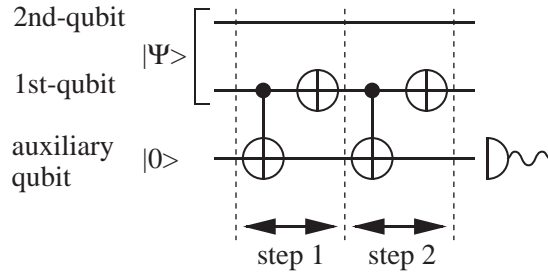
Figure 7: Eve's Intercept/Resend attack on the system S.

$$\forall\ L_1, L_2 \in \{\boldsymbol{I}, H, \sigma_x, H\sigma_x\}, \qquad \forall\ a \in \{0, 1\}$$
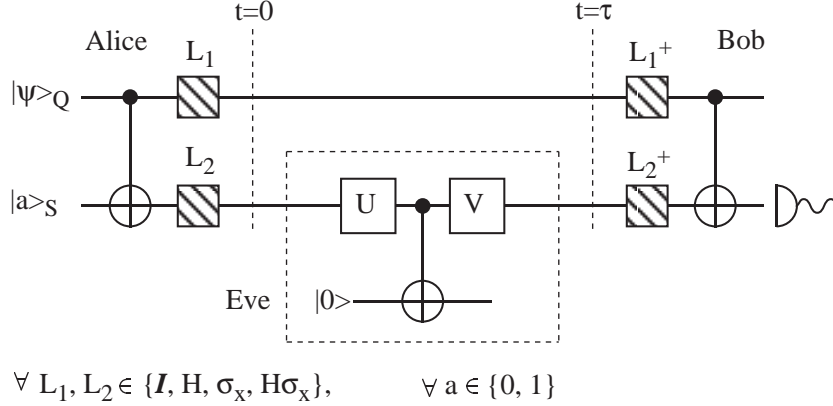
$$\xrightarrow{\text{step 2}} \sum_i (c_{i0}|i\rangle_2|0\rangle_1 + c_{i1}|i\rangle_2|1\rangle_1)|1\rangle_A$$

$$= |\Psi\rangle_Q|1\rangle_A.$$

Therefore, measuring an auxiliary system as shown in Figures 5 and 6 for each channel, Bob can examine whether all of the qubits are arrived or not.

4 Security against eavesdropping

It is difficult to consider all strategies Eve may take. In this section, we assume Eve to make only the Intercept/Resend attack. Eve measures each transmitted qubit with a proper basis independently and sends an alternative one according to the result of the measurement[2]. We pay attention to the following fact. Eve cannot extract information about $|\Psi\rangle_Q$ at all without getting the first password $\boldsymbol{i}$ of $U_{\boldsymbol{i}}^Q|\Psi\rangle_Q$, because the enciphered density operator is in proportion to $\boldsymbol{I}$ for her. Therefore, Eve needs to keep her illegal action secret from Alice and Bob during their authentication process so that Alice may disclose the first password $\boldsymbol{i}$. In this section, we estimate a probability that Alice and Bob fail to notice Eve's illegal act.

For simplicity, we assume that $|\Psi\rangle_Q$ is an arbitrary n-qubit product state for a while. At the first encryption, Alice applies $\forall U_{\boldsymbol{i}}^Q = \sigma_{i_1} \otimes \cdots \otimes \sigma_{i_n}$ to $|\Psi\rangle_Q = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$. Hence, $U_{\boldsymbol{i}}^Q|\Psi\rangle_Q$ is also a product state and we may treat each qubit independently.

We write the kth qubit ($\forall k \in \{1, \cdots, n\}$) of $U_{\boldsymbol{i}}^Q|\Psi\rangle_Q$ as $|\psi\rangle_Q = \alpha|0\rangle_Q + \beta|1\rangle_Q$ and the kth qubit of the signature as $|a\rangle_S$ ($a \in \{0, 1\}$). A state that Alice sends at $t = 0$ in Figure 7 is given by

$$\alpha L_1|0\rangle_Q L_2|a\rangle_S + \beta L_1|1\rangle_Q L_2|a \oplus 1\rangle_S.$$

Bob measures only the system S at $t = \tau$. If he gets $|a\rangle_S$, Alice and Bob consider the state is transmitted correctly. Bob uses the following projection operator for the measurement,

$$\Pi_{L_1,L_2}^{QS} = (L_1|0\rangle\langle 0|L_1^\dagger)_Q \otimes (L_2|a\rangle\langle a|L_2^\dagger)_S + (L_1|1\rangle\langle 1|L_1^\dagger)_Q \otimes (L_2|a \oplus 1\rangle\langle a \oplus 1|L_2^\dagger)_S.$$

Figure 8: Eve's Intercept/Resend attack on one qubit.

$|\phi>_S$ ──U──●──V──⊡〰

$|0>_E$ ────────⊕────────

$|\phi>_S = L_2|0>_S$

$L_2 \in \{I, H, \sigma_x, H\sigma_x\}$

Here, we assume Eve makes an attack only on the qubit of the system S as Figure 7 (U and V are arbitrary unitary transformations applied to one qubit). We write the dynamical process of S as a completely positive linear map \$ that represents Eve's Intercept/Resend attack on S[14]. Hence, the density operator ρ^S at $t = 0$ evolves to $\$(\rho^S)$ at $t = \tau$. We can write the state of QS at $t = \tau$ as

$$
\begin{aligned}
\rho_{L_1,L_2}^{QS}(\tau) &= |\alpha|^2 (L_1|0\rangle\langle 0|L_1^\dagger)_Q \otimes \$(L_2|a\rangle\langle a|L_2^\dagger)_S \\
&+ \alpha\beta^* (L_1|0\rangle\langle 1|L_1^\dagger)_Q \otimes \$(L_2|a\rangle\langle a \oplus 1|L_2^\dagger)_S \\
&+ \beta\alpha^* (L_1|1\rangle\langle 0|L_1^\dagger)_Q \otimes \$(L_2|a \oplus 1\rangle\langle a|L_2^\dagger)_S \\
&+ |\beta|^2 (L_1|1\rangle\langle 1|L_1^\dagger)_Q \otimes \$(L_2|a \oplus 1\rangle\langle a \oplus 1|L_2^\dagger)_S.
\end{aligned}
$$

We can write the probability P that Bob obtains $|a\rangle_S$ as

$$
\begin{aligned}
P &= \mathrm{Tr}_{QS}[\rho_{L_1,L_2}^{QS}(\tau)\Pi_{L_1,L_2}^{QS}] \\
&= |\alpha|^2\langle a|L_2^\dagger\$(L_2|a\rangle\langle a|L_2^\dagger)L_2|a\rangle + |\beta|^2\langle a \oplus 1|L_2^\dagger\$(L_2|a \oplus 1\rangle\langle a \oplus 1|L_2^\dagger)L_2|a \oplus 1\rangle. \quad (5)
\end{aligned}
$$

Seeing this, we find the following fact. Although the initial state $|\psi\rangle_Q$ of the system Q is a superposition of $|0\rangle$ and $|1\rangle$, we may regard the state as a mixed state of $|\psi\rangle_Q = |0\rangle$ and $|\psi\rangle_Q = |1\rangle$ with classical probability for evaluating P.

Therefore, the probability of Bob's authentication is equal to an average of probabilities that a network of quantum gates in Figure 8 gives $|\phi\rangle_S$ as an outcome from an incoming state $|\phi\rangle_S = L_2|0\rangle_S$ for all of $L_2 \in \mathcal{L}$. Here, we evaluate P as follows. U and V are arbitrary unitary transformations applied to one qubit. We assume U is defined as

$$
U|\varphi_0\rangle = |0\rangle, \qquad U|\varphi_1\rangle = |1\rangle,
$$

where $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ is a certain orthonormal basis of $\mathcal{H}_2$. Then, we write $|\phi\rangle = c_0|\varphi_0\rangle + c_1|\varphi_1\rangle$. The state is transformed on the network of Figure 8 as

$$
\begin{aligned}
|\phi\rangle_S|0\rangle_E &= (c_0|\varphi_0\rangle_S + c_1|\varphi_1\rangle_S)|0\rangle_E \\
&\xrightarrow{U} (c_0|0\rangle_S + c_1|1\rangle_S)|0\rangle_E \\
&\xrightarrow{\text{C-NOT}} c_0|0\rangle_S|0\rangle_E + c_1|1\rangle_S|1\rangle_E \\
&\xrightarrow{V} c_0V|0\rangle_S|0\rangle_E + c_1V|1\rangle_S|1\rangle_E. \quad (6)
\end{aligned}
$$

Seeing Eq. (6), we find that Eve measures the enciphered qubit in the basis $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ and sends a ket vector of a basis $\{V|0\rangle, V|1\rangle\}$ according to a result of measurement.

Hence, we can write the probability P_ϕ that Bob gets the correct signature for $|\phi\rangle_S$ in spite of Eve's illegal act as

$$P_\phi = |c_0|^2 |\langle\phi|V|0\rangle|^2 + |c_1|^2 |\langle\phi|V|1\rangle|^2. \tag{7}$$

From now on, for simplicity, we write equations with density operators. Defining

$$\rho_\phi = |\phi\rangle\langle\phi|, \quad \tilde{\rho}_0 = |\varphi_0\rangle\langle\varphi_0|, \quad \tilde{\rho}_1 = |\varphi_1\rangle\langle\varphi_1|, \quad \tilde{\rho}'_0 = V|0\rangle\langle 0|V^\dagger, \quad \tilde{\rho}'_1 = V|1\rangle\langle 1|V^\dagger,$$

we can write Eq. (6) as

$$\rho_\phi \to \$(\rho_\phi) = (\mathrm{Tr}\rho_\phi\tilde{\rho}_0)\tilde{\rho}'_0 + (\mathrm{Tr}\rho_\phi\tilde{\rho}_1)\tilde{\rho}'_1,$$

and Eq. (7) as

$$P_\phi = \mathrm{Tr}[\$(\rho_\phi)\rho_\phi].$$

Four density operators $L_2|0\rangle\langle 0|L_2^\dagger$ ($L_2 \in \mathcal{L}$), emitted as $|\phi\rangle_S$ with equal probability, are described as

$$\rho_\updownarrow = \frac{1}{2}(\boldsymbol{I} + \sigma_z), \quad \rho_\leftrightarrow = \frac{1}{2}(\boldsymbol{I} - \sigma_z), \quad \rho_\circlearrowleft = \frac{1}{2}(\boldsymbol{I} + \sigma_x), \quad \rho_\circlearrowright = \frac{1}{2}(\boldsymbol{I} - \sigma_x).$$

Then we define

$$\tilde{\rho}_i = \frac{1}{2}[\boldsymbol{I} + (-1)^i \boldsymbol{X} \cdot \boldsymbol{\sigma}], \quad \tilde{\rho}'_j = \frac{1}{2}[\boldsymbol{I} + (-1)^j \boldsymbol{X}' \cdot \boldsymbol{\sigma}] \quad \text{for } i,j \in \{0,1\},$$

where $\boldsymbol{X} = (X,Y,Z)$ and $\boldsymbol{X}' = (X',Y',Z')$ are arbitrary three-component real vectors with $|\boldsymbol{X}|^2 = |\boldsymbol{X}'|^2 = 1$. Using the following formula,

$$\mathrm{Tr}(\boldsymbol{I} + \boldsymbol{A} \cdot \boldsymbol{\sigma})(\boldsymbol{I} + \boldsymbol{B} \cdot \boldsymbol{\sigma}) = 2(1 + \boldsymbol{A} \cdot \boldsymbol{B}),$$

and averaging four kinds of P_ϕ, we estimate P_B that Bob measures the correct signature in spite of Eve's illegal act at

$$P_B = \frac{1}{4}(P_\updownarrow + P_\leftrightarrow + P_\circlearrowleft + P_\circlearrowright) = \frac{1}{4}(2 + XX' + ZZ') \leq \frac{3}{4}. \tag{8}$$

Therefore, the probability that Alice and Bob do not notice Eve make an attack by the network of Figure 8 is 3/4 or less. If Eve makes the Intercept/Resend attack on the system Q, we can give a similar discussion. Consequently, the probability that Alice and Bob do not notice Eve's attacks on m qubits (either Q or S in each pair) is $(3/4)^m$ at most.

Next, we consider the case that Eve makes the Intercept/Resend attack on both qubits of a pair QS independently in Figure 9 (U_1, U_2, V_1, and V_2 are arbitrary unitary transformations). Measuring ρ^{QS} transmitted from Alice, Eve sends the following density operator $\rho^{QS'}$ to Bob,

$$\rho^{QS'} = \$(\rho^{QS}) = \sum_{i,j \in \{0,1\}} \mathrm{Tr}(\rho^{QS} \tilde{\rho}_{Q,i} \tilde{\rho}_{S,j}) \tilde{\rho}'_{Q,i} \tilde{\rho}'_{S,j},$$

13

Figure 9: Eve's Intercept/Resend attack on the system Q and S.
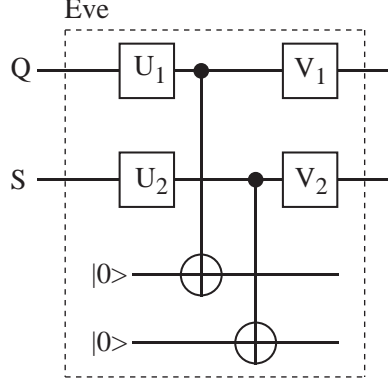
where

$$
\begin{aligned}
\tilde{\rho}_{Q,i} &= U_1^{\dagger}|i\rangle\langle i|U_1 &= (1/2)[\boldsymbol{I} + (-1)^i \boldsymbol{X}_1 \cdot \boldsymbol{\sigma}], \\
\tilde{\rho}_{S,j} &= U_2^{\dagger}|j\rangle\langle j|U_2 &= (1/2)[\boldsymbol{I} + (-1)^j \boldsymbol{X}_2 \cdot \boldsymbol{\sigma}], \\
\tilde{\rho}'_{Q,i} &= V_1|i\rangle\langle i|V_1^{\dagger} &= (1/2)[\boldsymbol{I} + (-1)^i \boldsymbol{X}_3 \cdot \boldsymbol{\sigma}], \\
\tilde{\rho}'_{S,j} &= V_2|j\rangle\langle j|V_2^{\dagger} &= (1/2)[\boldsymbol{I} + (-1)^j \boldsymbol{X}_4 \cdot \boldsymbol{\sigma}],
\end{aligned}
\tag{9}
$$

and $|\boldsymbol{X}_k|^2 = 1 \ (k = 1, \cdots, 4)$.

Here, we can assume $|a\rangle_S$ to be $|0\rangle_S$ without losing generality. We write a transmitted state of Q as $|\psi\rangle_Q = \alpha|0\rangle + \beta|1\rangle$. Because Alice has sixteen kinds of ways to send the state for $L_1, L_2 \in \mathcal{L}$, Bob's final probability for authentication is described as

$$
P_B = \frac{1}{16} \sum_{L_1, L_2 \in \mathcal{L}} \mathrm{Tr}[\$(\rho_{L_1,L_2}^{QS})\Pi_{L_1,L_2}^{QS}].
\tag{10}
$$

Writing the density operator of the state $\alpha L_1|0\rangle_Q L_2|0\rangle_S + \beta L_1|1\rangle_Q L_2|1\rangle_S$ that Alice sends to Bob as ρ_{L_1,L_2}^{QS}, we can describe its explicit form as

$$
\begin{aligned}
\rho_{L_1,L_2}^{QS} &= |\alpha|^2 (L_1|0\rangle\langle 0|L_1^{\dagger})_Q \otimes (L_2|0\rangle\langle 0|L_2^{\dagger})_S \\
&\quad + \alpha\beta^*(L_1|0\rangle\langle 1|L_1^{\dagger})_Q \otimes (L_2|0\rangle\langle 1|L_2^{\dagger})_S + \beta\alpha^*(L_1|1\rangle\langle 0|L_1^{\dagger})_Q \otimes (L_2|1\rangle\langle 0|L_2^{\dagger})_S \\
&\quad + |\beta|^2 (L_1|1\rangle\langle 1|L_1^{\dagger})_Q \otimes (L_2|1\rangle\langle 1|L_2^{\dagger})_S.
\end{aligned}
\tag{11}
$$

The projection operator for Bob is given by

$$
\Pi_{L_1,L_2}^{QS} = (L_1|0\rangle\langle 0|L_1^{\dagger})_Q \otimes (L_2|0\rangle\langle 0|L_2^{\dagger})_S + (L_1|1\rangle\langle 1|L_1^{\dagger})_Q \otimes (L_2|1\rangle\langle 1|L_2^{\dagger})_S.
$$

Eq. (10) is linear for ρ_{L_1,L_2}^{QS}. Therefore, we can divide Eq. (11) into terms for calculation.

First, we think about the first and forth terms of Eq. (11). We write the first term as

$$
\varrho_{L_1,L_2}^{QS} = (L_1|0\rangle\langle 0|L_1^{\dagger})_Q \otimes (L_2|0\rangle\langle 0|L_2^{\dagger})_S.
\tag{12}
$$

For example, if $L_1 = L_2 = \boldsymbol{I}$, we obtain

$$
\begin{aligned}
\varrho_{\boldsymbol{I},\boldsymbol{I}}^{QS} &= (1/4)(\boldsymbol{I} + \sigma_z)_Q \otimes (\boldsymbol{I} + \sigma_z)_S, \\
\Pi_{\boldsymbol{I},\boldsymbol{I}}^{QS} &= (1/4)[(\boldsymbol{I} + \sigma_z)_Q \otimes (\boldsymbol{I} + \sigma_z)_S + (\boldsymbol{I} - \sigma_z)_Q \otimes (\boldsymbol{I} - \sigma_z)_S],
\end{aligned}
$$

14

and
$$\mathrm{Tr}[\$(\varrho_{\boldsymbol{I},\boldsymbol{I}}^{QS})\Pi_{\boldsymbol{I},\boldsymbol{I}}^{QS}] = (1/2)(1 + Z_1 Z_2 Z_3 Z_4).$$

From similar calculations, we get

$$\mathrm{Tr}[\$(\varrho_{L_1,L_2}^{QS})\Pi_{L_1,L_2}^{QS}] = \begin{cases} (1/2)(1 + Z_1 Z_2 Z_3 Z_4) & \text{for } L_1, L_2 \in \{\boldsymbol{I}, \sigma_x\}, \\ (1/2)(1 + X_1 X_2 X_3 X_4) & \text{for } L_1, L_2 \in \{H, H\sigma_x\}, \\ (1/2)(1 + Z_1 X_2 Z_3 X_4) & \text{for } L_1 \in \{\boldsymbol{I}, \sigma_x\},\ L_2 \in \{H, H\sigma_x\}, \\ (1/2)(1 + X_1 Z_2 X_3 Z_4) & \text{for } L_1 \in \{H, H\sigma_x\},\ L_2 \in \{\boldsymbol{I}, \sigma_x\}. \end{cases}$$

Therefore, we obtain

$$\frac{1}{16}\sum_{L_1,L_2} \mathrm{Tr}[\$(\varrho_{L_1,L_2}^{QS})\Pi_{L_1,L_2}^{QS}] = \frac{1}{2} + \frac{1}{8}(X_1 X_3 + Z_1 Z_3)(X_2 X_4 + Z_2 Z_4).$$

Next, we think about the second and third terms of Eq. (11). We write the second term as

$$\Delta\varrho_{L_1,L_2}^{QS} = (L_1|0\rangle\langle 1|L_1^\dagger)_Q \otimes (L_2|0\rangle\langle 1|L_2^\dagger)_S.$$

For example, if $L_1 = L_2 = \boldsymbol{I}$, we obtain

$$\begin{aligned}
\Delta\varrho_{\boldsymbol{I},\boldsymbol{I}}^{QS} &= (1/4)(\sigma_x + i\sigma_y)_Q \otimes (\sigma_x + i\sigma_y)_S, \\
\mathrm{Tr}[\$(\Delta\varrho_{\boldsymbol{I},\boldsymbol{I}}^{QS})\Pi_{\boldsymbol{I},\boldsymbol{I}}^{QS}] &= (1/2)(X_1 + iY_1)(X_2 + iY_2)Z_3 Z_4.
\end{aligned}$$

From similar calculations, we get

$$\mathrm{Tr}[\$(\Delta\varrho_{L_1,L_2}^{QS})\Pi_{L_1,L_2}^{QS}]$$

$$= \begin{cases}
(1/2)[X_1 + i\epsilon Y_1][X_2 + i\epsilon Y_2]Z_3 Z_4 & (L_1, L_2) = (\boldsymbol{I},\boldsymbol{I}), & (\sigma_x, \sigma_x), \\
-(1/2)[X_1 + i\epsilon Y_1][X_2 - i\epsilon Y_2]Z_3 Z_4 & (\boldsymbol{I}, \sigma_x), & (\sigma_x, \boldsymbol{I}), \\
(1/2)[Z_1 - i\epsilon Y_1][Z_2 - i\epsilon Y_2]X_3 X_4 & (H, H), & (H\sigma_x, H\sigma_x), \\
-(1/2)[Z_1 - i\epsilon Y_1][Z_2 + i\epsilon Y_2]X_3 X_4 & (H, H\sigma_x), & (H\sigma_x, H), \\
(1/2)[X_1 + i\epsilon Y_1][Z_2 - i\epsilon Y_2]Z_3 X_4 & (\boldsymbol{I}, H), & (\sigma_x, H\sigma_x), \\
-(1/2)[X_1 + i\epsilon Y_1][Z_2 + i\epsilon Y_2]Z_3 X_4 & (\boldsymbol{I}, H\sigma_x), & (\sigma_x, H), \\
(1/2)[Z_1 - i\epsilon Y_1][X_2 + i\epsilon Y_2]X_3 Z_4 & (H, \boldsymbol{I}), & (H\sigma_x, \sigma_x), \\
-(1/2)[Z_1 - i\epsilon Y_1][X_2 - i\epsilon Y_2]X_3 Z_4 & (H, \sigma_x), & (H\sigma_x, \boldsymbol{I}).
\end{cases}$$

with column headers $\epsilon = 1$ and $\epsilon = -1$.

Consequently, we obtain

$$\frac{1}{16}\sum_{L_1,L_2} \mathrm{Tr}[\$(\Delta\varrho_{L_1,L_2}^{QS})\Pi_{L_1,L_2}^{QS}] = -\frac{1}{8}Y_1 Y_2 (Z_3 - X_3)(Z_4 - X_4).$$

Finally, obtaining

$$P_B = \frac{1}{2} + \frac{1}{8}(X_1 X_3 + Z_1 Z_3)(X_2 X_4 + Z_2 Z_4) - \frac{1}{8}(\alpha\beta^* + \alpha^*\beta)Y_1 Y_2 (Z_3 - X_3)(Z_4 - X_4), \quad (13)$$

we can show $P_B \leq 3/4$. (See Appendix A.) Therefore, if $|\Psi\rangle_Q$ is an n-qubit product state and if Eve makes the Intercept/Resend attack on both qubits of a pair QS independently

15

as Figure 9, the probability that Eve's illegal acts cannot be found is equal to 3/4 or less per one qubit.

Especially, if the transmitted information is classical, $|\Psi\rangle_Q$ is a product state of $|0\rangle$ and $|1\rangle$. All of the $2n$ qubits transmitted are in states chosen from four ket vectors of two conjugate bases at random. If we regard $\boldsymbol{a}$ as a key of an n-bit random string and $|\Psi\rangle_Q$ as an n-bit enciphered classical message, our method is equivalent to the one-time pad method with BB84. Assuming Eve makes attacks on m pairs of qubits in QS, we can estimate the probability of Eve's success in eavesdropping at $(3/4)^m$ or less.

Then, we consider the case that $|\Psi\rangle_Q$ is an arbitrary entangled state of n qubits. The enciphered state of $|\Psi\rangle_Q$ with $U_{\boldsymbol{i}}^Q$ is also entangled and it is given by Eq. (4).

First, we consider that Eve makes the Intercept/Resend attack on either one in a pair of qubits of the system Q and S as Figure 7. If Eve makes this attack on m pairs out of n pairs of the system QS, we can regard the transmission as sending an ensemble of product states, where each qubit is $|0\rangle$ or $|1\rangle$, with classical probabilities, like Eq. (5). We can think in a similar way before and conclude that the probability Eve's illegal act cannot be found is $(3/4)^m$ or less.

Next, we consider the case that Eve makes the attack on both qubits of a pair on the entangled system QS as Figure 9. If Eve makes this attack on m pairs out of n pairs, we can write the probability Eve is not found as an equation which is similar to Eq. (13) and it is estimated at $(3/4)^m$ or less. (See Appendix B.)

5   Privacy amplification process

From previous discussion, we obtain the following results. If an arbitrary quantum state is enciphered by our method, a probability that Alice and Bob do not notice Eve is at most 3/4 per one qubit. (Both product and entangled states are available. We assume that Eve always makes eavesdropping with the Intercept/Resend attack.) Hence, if Eve makes attacks on m enciphered pairs, her success probability is given by $(3/4)^m$ and it decreases exponentially against m.

However, there is a problem. In our method, if Eve replaces a pair of enciphered qubits with a pair of random ones, Alice and Bob do not notice her illegal act with probability of 1/2. In this case, they disclose passwords and Eve obtains one qubit of original information with fidelity 1. It is important that Eve gets a correct qubit and she knows that she obtains the correct one.

Such a problem can be also occurred in the BB84. It is possible that Alice and Bob share the same random binary string and Eve knows a few bits of it exactly. To overcome this trouble, for example, Alice and Bob can choose some bits at random from the shared binary string and make a new bit from a summation of them with modulo 2[2]. If they repeat this process and create a new binary string that is shorter than original one, Eve's expected information decreases to 0 in some asymptotic limit. Such a technique is called privacy amplification.

On the other hand, in our protocol, Eve's success probability for eavesdropping on one-qubit cannot always reach 0. To decrease it to 0 asymptotically, Alice and Bob apply our protocol over and over again. To make discussion simple, we consider encryption of

one-qubit quantum information for a while.

Preparing an arbitrary one-qubit state $|\psi_1\rangle$ and a one-qubit signature $|a_1\rangle$ ($\forall a_1 \in \{0, 1\}$), Alice applies our protocol to $|\psi_1\rangle|a_1\rangle$ and generates an entangled two-qubit state $|\psi_2\rangle$. Then, she prepares other qubits $|a_2\rangle|a_3\rangle$ for a signature, and enciphers $|\psi_2\rangle|a_2\rangle|a_3\rangle$ again. She obtains a four-qubit state $|\psi_3\rangle$.

If Eve wants to get quantum information of $|\psi_1\rangle$ with fidelity 1, she has to interact with all four qubits of $|\psi_3\rangle$. For example, if Eve replaces $|\psi_3\rangle$ with random four qubits, Alice and Bob notice her illegal act with probability of $(1/2)^3 = 1/8$, because they carry out the authentication process with $|a_1\rangle$, $|a_2\rangle$, and $|a_3\rangle$.

If Alice enciphers $|\psi_1\rangle$ for n times, the nth encryption needs 2^{n-1} signature qubits. If Eve makes attacks on all enciphered qubits of $|\psi_{n+1}\rangle$, the probability that Alice and Bob do not notice her act is $(3/4)^{N/2}$ at most, where $N = 2^n$ is the number of all enciphered qubits. (The probability $3/4$ comes from the fact that Alice enciphers the state with rectilinear and circular bases at random, and it does not depend on $|\psi_n\rangle$.) Hence, Eve's success probability that she gets $|\psi_1\rangle$ with fidelity of 1 decreases exponentially against the number of qubits, and reaches 0 in the limit of $N \to \infty$.

Another method is as follows. Alice and Bob share a random binary string beforehand as the first password (subscripts of Pauli matrices) in secrecy by BB84. Because they do not need to disclose it, Eve can never get information of $|\psi_1\rangle$ at all even in the case that they do not notice Eve's disturbance. In this method, the privacy amplification has to be done for BB84 actually.

6   Discussion

To understand our method more clearly, we consider a simple one and compare it with ours. For transmitting an n-qubit quantum state in secrecy, we can take the following method. Enciphering an n-qubit state ρ_n as Eq. (3), Alice prepares other n qubits as check ones that are given as $\{|0\rangle, |1\rangle\}$ or $\{(1/\sqrt{2})(|0\rangle \pm |1\rangle)\}$ at random respectively. Then, Alice permutes all of the $2n$ qubits at random and sends them to Bob.

Here, we assume Eve tries to eavesdrop on only one qubit of ρ_n. Because Eve does not know which qubits are check ones, a probability that Alice and Bob fail to notice Eve's illegal act can be $(1/2)[1 + (3/4)] = 7/8$ as the maximum, in spite of $3/4$ for our method. This is because we use entanglement in our method.

Even if Eve prepares an arbitrary one-qubit state by herself in spite of taking away a qubit from ρ_n, its expectation value of fidelity is equal to $1/2$. This shows that Eve's success probability of eavesdropping is always equal to $1/2$ or more. In our method, if Eve interacts enciphered qubits, a probability of her success is equal to at most $3/4$ per one qubit (without privacy amplification). It is similar to the BB84.

In this paper, the security against Eve's attack with using entanglement is not considered (for example, a case that she uses a quantum computer for eavesdropping as Figure 10). In Figure 10, it is difficult to evaluate the upper bound of the probability that Bob measures the signature correctly for arbitrary unitary transformations U_1, U_2,

Figure 10: Eve's attack on the system QS by using entanglement.
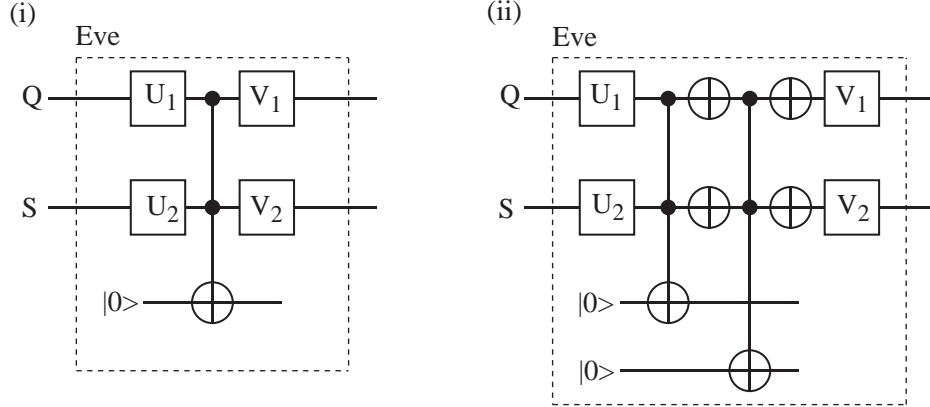
V_1, and V_2. For instance, assuming

$$U_1 = U_2 = V_1 = V_2 = U \qquad \text{where } U = \begin{pmatrix} \cos(\pi/8) & \sin(\pi/8) \\ \sin(\pi/8) & -\cos(\pi/8) \end{pmatrix},$$

and $|\Psi\rangle_Q$ represents classical information (an n-qubit product state of $|0\rangle$ and $|1\rangle$), we get $P_B = (13/16) > (3/4)$ for Figure 10. i and $P_B = (11/16) < (3/4)$ for Figure 10. ii. Eavesdropping with U is equivalent to measuring and resending a qubit in the following basis,

$$|\varphi_i\rangle\langle\varphi_i| = \frac{1}{2}(\boldsymbol{I} + (-1)^i \boldsymbol{X} \cdot \boldsymbol{\sigma}), \qquad \boldsymbol{X} = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}),$$

which is called the Breidbart basis[2]. About Figure 10. i, P_B may exceed $3/4$. But, the amount of information Eve can extract in Figure 10. i seems to be less than the amount of information she obtains by the Intercept/Resend attack on one qubit as Figure 7.

In our method, if Eve takes away qubits, Alice and Bob lose original information of them.

We mentioned in Sec. 1 that the classical key distribution can be done only by the uncertainty, and the entanglement is not essential for it[3][4]. On the other hand, for transmitting quantum states by the quantum teleportation, the entanglement plays an essential role[6]. Our method uses both two properties.

Recently, the method for transmitting classical binary data (not a classical random string) in secrecy with a pair of entangled photons has been proposed[15]. It is characterized by the following facts. First, Alice and Bob prepare two conjugate bases on $\mathcal{H}_2^2$ each for encoding message and measuring photons. Second, they use a two-dimensional subspace of $\mathcal{H}_2^2$ for encoding a binary digit.

Acknowledgements

A   The maximum value of P_B for a product state $|\Psi\rangle_Q$

Here, we show that P_B defined in Eq. (13) never exceeds $3/4$.

Because of $|\alpha|^2 + |\beta|^2 = 1$, we get $-1 \leq \alpha\beta^* + \alpha^*\beta \leq 1$. Hence, altering the signs of X_i as $X_i \rightarrow -X_i$ $(i = 1, \cdots, 4)$, we can write the upper bound of P_B as

$$P_B \leq \frac{1}{2} + \frac{1}{8}f_{MAX},$$

where f_{MAX} is the maximum value of

$$f = (X_1 X_3 + Z_1 Z_3)(X_2 X_4 + Z_2 Z_4) + Y_1 Y_2 (X_3 + Z_3)(X_4 + Z_4), \tag{14}$$

with $|\boldsymbol{X}_i|^2 = 1$ and $X_i, Y_i, Z_i \geq 0$ for $i = 1, \cdots, 4$.

Seeing Eq. (14), we give another form of f as follows,

$$f = |\boldsymbol{A} \cdot \boldsymbol{B}|,$$

where

$$\begin{aligned}
\boldsymbol{A} &= (X_1 X_3 + Z_1 Z_3, Y_1(X_3 + Z_3)), \\
\boldsymbol{B} &= (X_2 X_4 + Z_2 Z_4, Y_2(X_4 + Z_4)).
\end{aligned}$$

(We pay an attention that $\boldsymbol{A}$ and $\boldsymbol{B}$ are two-component real vectors.) From the Cauchy-Schwarz inequality, we get

$$f \leq |\boldsymbol{A}||\boldsymbol{B}|.$$

Therefore, by estimating the maximum values of $|\boldsymbol{A}|$ and $|\boldsymbol{B}|$, we derive the upper bound of f.

We can write $|\boldsymbol{A}|^2$ in the following form,

$$|\boldsymbol{A}|^2 = (1 - Z_1^2)X_3^2 + (1 - X_1^2)Z_3^2 + 2(X_1 Z_3)(Z_1 X_3) + 2Y_1^2(X_3 Z_3).$$

On the other hand, from the arithmetic-geometric inequality, we obtain

$$\begin{aligned}
(X_1 Z_3)(Z_1 X_3) &\leq \frac{1}{2}[(X_1 Z_3)^2 + (Z_1 X_3)^2], \\
X_3 Z_3 &\leq \frac{1}{2}(X_3^2 + Z_3^2).
\end{aligned}$$

Therefore, we get

$$|\boldsymbol{A}|^2 \leq (1 + Y_1^2)(X_3^2 + Z_3^2) \leq 1 + Y_1^2 \leq 2. \tag{15}$$

We obtain $|\boldsymbol{A}| \leq \sqrt{2}$. In a similar way, we obtain $|\boldsymbol{B}| \leq \sqrt{2}$. From these results, we can conclude that $f \leq 2$ and $f_{MAX} = 2$.

B The maximum value of P_B for an entangled state $|\Psi\rangle_Q$

We estimate the probability that Eve's illegal act cannot be found in the case where she makes the Intercept/Resend attack on m pairs of qubits on the system QS for an arbitrary entangled $|\Psi\rangle_Q$ of n qubits.

For simplicity, we assume $|\Psi\rangle_Q$ to be an arbitrary entangled state of two-qubit system qq' at first,

$$|\Psi\rangle_Q = \sum_{i,j \in \{0,1\}} c_{ij} |i\rangle_q \otimes |j\rangle_{q'} \in \forall \mathcal{H}_2^2.$$

Alice puts two qubits of the system $S(= ss')$ for the signature on the qubits of the system $Q(= qq')$ respectively. Then, she makes entanglement between the systems Q and S with C-NOT gates, applies L_1, L_2, L_1', $L_2' \in \mathcal{L}$ to four qubits q, s, q', s' respectively, and sends them to Bob (see Figure 7). Eve makes the Intercept/Resend attacks on the systems q, s, q', s' respectively as shown in Figure 9. We can assume the initial states of qubits s, s' that represents the signature to be $|0\rangle_s |0\rangle_{s'}$ without losing generality.

Writing the state sent by Alice as

$$\sum_{i,j \in \{0,1\}} c_{ij} L_1 |i\rangle_q L_2 |i\rangle_s \otimes L_1' |j\rangle_{q'} L_2' |j\rangle_{s'},$$

we can describe the density operator explicitly as

$$
\begin{aligned}
\rho^{QS}_{L_1 L_2 L_1' L_2'} &= (L_1 L_2 L_1' L_2') \sum_{i,j \in \{0,1\}} [|c_{ij}|^2 (|i\rangle\langle i|_q \otimes |i\rangle\langle i|_s) \otimes (|j\rangle\langle j|_{q'} \otimes |j\rangle\langle j|_{s'}) \\
&\quad + c_{ij} c_{i\bar{j}}^* (|i\rangle\langle i|_q \otimes |i\rangle\langle i|_s) \otimes (|j\rangle\langle \bar{j}|_{q'} \otimes |j\rangle\langle \bar{j}|_{s'}) \\
&\quad + c_{ij} c_{\bar{i}j}^* (|i\rangle\langle \bar{i}|_q \otimes |i\rangle\langle \bar{i}|_s) \otimes (|j\rangle\langle j|_{q'} \otimes |j\rangle\langle j|_{s'}) \\
&\quad + c_{ij} c_{\bar{i}\bar{j}}^* (|i\rangle\langle \bar{i}|_q \otimes |i\rangle\langle \bar{i}|_s) \otimes (|j\rangle\langle \bar{j}|_{q'} \otimes |j\rangle\langle \bar{j}|_{s'})] (L_1 L_2 L_1' L_2')^\dagger, \quad (16)
\end{aligned}
$$

where $\bar{i} = i + 1 \pmod 2$.

Eavesdropping on the state $\rho^{QS}_{L_1 L_2 L_1' L_2'}$, Eve transforms it to the following state,

$$\$(\rho^{QS}_{L_1 L_2 L_1' L_2'}) = \sum_{i,j,k,l \in \{0,1\}} \mathrm{Tr}(\rho^{QS}_{L_1 L_2 L_1' L_2'} \tilde{\rho}_{q,i} \tilde{\rho}_{s,j} \tilde{\rho}_{q',k} \tilde{\rho}_{s',l}) \tilde{\rho}'_{q,i} \tilde{\rho}'_{s,j} \tilde{\rho}'_{q',k} \tilde{\rho}'_{s',l}.$$

where

$$
\begin{array}{llll}
\tilde{\rho}_{q,i} &= (1/2)[\boldsymbol{I} + (-1)^i \boldsymbol{X}_1 \cdot \boldsymbol{\sigma}], & \tilde{\rho}_{s,j} &= (1/2)[\boldsymbol{I} + (-1)^j \boldsymbol{X}_2 \cdot \boldsymbol{\sigma}], \\
\tilde{\rho}'_{q,i} &= (1/2)[\boldsymbol{I} + (-1)^i \boldsymbol{X}_3 \cdot \boldsymbol{\sigma}], & \tilde{\rho}'_{s,j} &= (1/2)[\boldsymbol{I} + (-1)^j \boldsymbol{X}_4 \cdot \boldsymbol{\sigma}], \\
\tilde{\rho}_{q',k} &= (1/2)[\boldsymbol{I} + (-1)^k \boldsymbol{X}_1' \cdot \boldsymbol{\sigma}], & \tilde{\rho}_{s',l} &= (1/2)[\boldsymbol{I} + (-1)^l \boldsymbol{X}_2' \cdot \boldsymbol{\sigma}], \\
\tilde{\rho}'_{q',k} &= (1/2)[\boldsymbol{I} + (-1)^k \boldsymbol{X}_3' \cdot \boldsymbol{\sigma}], & \tilde{\rho}'_{s',l} &= (1/2)[\boldsymbol{I} + (-1)^l \boldsymbol{X}_4' \cdot \boldsymbol{\sigma}],
\end{array}
\quad (17)
$$

and $|\boldsymbol{X}_k|^2 = |\boldsymbol{X}_k'|^2 = 1$ $(k = 1, \cdots, 4)$. Bob measures it with the projection operator,

$$
\begin{aligned}
\Pi^{QS}_{L_1 L_2 L_1' L_2'} &= (L_1 L_2)(|0\rangle\langle 0|_q \otimes |0\rangle\langle 0|_s + |1\rangle\langle 1|_q \otimes |1\rangle\langle 1|_s)(L_1 L_2)^\dagger \\
&\quad \otimes (L_1' L_2')(|0\rangle\langle 0|_{q'} \otimes |0\rangle\langle 0|_{s'} + |1\rangle\langle 1|_{q'} \otimes |1\rangle\langle 1|_{s'})(L_1' L_2')^\dagger.
\end{aligned}
$$

The probability that Bob measures the correct signature is given by

$$
\begin{aligned}
P_B &= (\frac{1}{16})^2 \sum_{L_1,L_2\in\mathcal{L}} \sum_{L'_1,L'_2\in\mathcal{L}} \mathrm{Tr}[\$(\rho^{QS}_{L_1L_2L'_1L'_2})\Pi^{QS}_{L_1L_2L'_1L'_2}]\\
&= [\frac{1}{2} + \frac{1}{8}(X_1X_3 + Z_1Z_3)(X_2X_4 + Z_2Z_4)][\frac{1}{2} + \frac{1}{8}(X'_1X'_3 + Z'_1Z'_3)(X'_2X'_4 + Z'_2Z'_4)]\\
&\quad + \sum_{i,j\in\{0,1\}} \{c_{ij}c^*_{i\bar{j}}[\frac{1}{2} + \frac{1}{8}(X_1X_3 + Z_1Z_3)(X_2X_4 + Z_2Z_4)]\\
&\qquad\qquad \times[-\frac{1}{8}Y'_1Y'_2(Z'_3 - X'_3)(Z'_4 - X'_4)]\\
&\quad +c_{ij}c^*_{\bar{i}j}[-\frac{1}{8}Y_1Y_2(Z_3 - X_3)(Z_4 - X_4)][\frac{1}{2} + \frac{1}{8}(X'_1X'_3 + Z'_1Z'_3)(X'_2X'_4 + Z'_2Z'_4)]\\
&\quad +c_{ij}c^*_{\bar{i}\bar{j}}[-\frac{1}{8}Y_1Y_2(Z_3 - X_3)(Z_4 - X_4)][-\frac{1}{8}Y'_1Y'_2(Z'_3 - X'_3)(Z'_4 - X'_4)]\}.
\end{aligned}
$$

From $\sum_{i,j\in\{0,1\}} |c_{ij}|^2 = 1$, we obtain $|\sum_{i,j\in\{0,1\}} c_{ij}c^*_{i\bar{j}}| \leq 1$, $|\sum_{i,j\in\{0,1\}} c_{ij}c^*_{\bar{i}j}| \leq 1$, and $|\sum_{i,j\in\{0,1\}} c_{ij}c^*_{\bar{i}\bar{j}}| \leq 1$. Therefore, using the result obtained in Appendix A, we can conclude

$$
P_B \leq (\frac{1}{2} + \frac{1}{8}f_{MAX})^2 = (\frac{3}{4})^2.
$$

(We pay attention to a fact that each term of P_B can be gathered with a binomial coefficient.) When Eve attacks on m pairs out of enciphered qubits generated from an arbitrary n-qubit entangled state $|\Psi\rangle_Q$, we obtain $P_B \leq (3/4)^m$.

References

[1] C. H. Bennett and G. Brassard, 'Quantum cryptography : Public key distribution and coin tossing', Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175-179, December 1984.

[2] C. H. Bennett, F. B. Bessette, G. Brassard, L. Salvail and J. Smolin, 'Experimental Quantum Cryptography', J. Cryptology, **5** : 3-28 (1992).

[3] A. K. Ekert, 'Quantum Cryptography Based on Bell's Theorem', Phys. Rev. Lett. **67**, 661 (1991).

[4] C. H. Bennett, G. Brassard, and N. D. Mermin, 'Quantum Cryptography without Bell's Theorem', Phys. Rev. Lett. **68**, 557 (1992).

[5] C. H. Bennett, G. Brassard and A. K. Ekert, 'Quantum Cryptography', Scientific American, **267**, No. 4, 50-57, October 1992.

[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, 'Teleporting an unknown quantum states via dual classic and Einstein-Podolsky-Rosen channels', Phys. Rev. Lett. **70**, 1895 (1993).

[7] D. Bouwmeester, J-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, 'Experimental quantum teleportation', Nature **390**, 575-579 (1997).
A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble and E. S. Polzik, 'Unconditional Quantum Teleportation', Science **282**, 706-709 (1998).

[8] W. K. Wootters and W. H. Zurek, 'A single quantum cannot be cloned', Nature **299**, 802-803 (1982).

[9] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, 'Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels', Phys. Rev. Lett. **76**, 722 (1996).
D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, 'Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels', Phys. Rev. Lett. **77**, 2818 (1996).
C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, 'Mixed-state entanglement and quantum error correction', Phys. Rev. A **54**, 3824 (1996).

[10] R. P. Feynman, 'Feynman Lectures on Computation', Addison-Wesley (1996).
A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, 'Elementary gates for quantum computation', Phys. Rev. A **52**, 3457 (1995).

[11] I. L. Chuang and Y. Yamamoto, 'Simple quantum computer', Phys. Rev. A **52**, 3489 (1995).

[12] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi and J. Kimble, 'Measurement of conditional phase shifts for quantum logic', Phys. Rev. Lett. **75**, 4710 (1995).

[13] D. Gottesman, 'Stabilizer Codes and Quantum Error Correction', Ph. D. thesis, California Institute of Technology, LANL quantum physics archive **quant-ph/9705052**.

[14] B. Schumacher, 'Sending entanglement through noisy quantum channels', Phys. Rev. A **54**, 2614 (1996).
A. Fujiwara and P. Algoet, 'One-to-one parametrization of quantum channels', Phys. Rev. A **59**, 3290 (1999).

[15] K. Shimizu and N. Imoto, 'Communication channels secured from eavesdropping via transmission of photonic Bell states', Phys. Rev. A **60**, 157 (1999).

[16] D. Deutsch and R. Jozsa, 'Rapid solution of problems by quantum computation', Proc. R. Soc. Lond. A **439**, 553 (1992).
P. W. Shor, 'Algorithms for quantum computation: Discrete logarithms and factoring' in Proceedings of the 35th Annual Symposium on Foundations of Computer Science (ed. S. Goldwasser) 124-134 (IEEE Computer Society, Los Alamitos, CA, 1994).
P. W. Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', SIAM J. Computing **26**, 1484 (1997).

[17] P. O. Boykin and V. Roychowdhury, 'Optimal Encryption of Quantum Bits', LANL quantum physics archive **quant-ph/0003059**.
M. Mosca, A. Tapp and R. de Wolf, 'Private Quantum Channels and the Cost of Randomizing Quantum Information', LANL quantum physics archive **quant-ph/0003101**.